Seguridad Cibernética

¿Te has dado cuenta cómo las tecnologías de la información y las comunicaciones han transformado las sociedades en todo el mundo?

Las innovaciones han creado mercados nuevos de bienes y servicios, los procesos laborales se han revolucionado mejorando la productividad, ha aumentado la velocidad del flujo de capitales y las sociedades han experimentado cambios culturales.

Este crecimiento exponencial en las nuevas tecnologías de la información y las comunicaciones por el otro lado, ha posibilitado nuevas formas de explotación, nuevas oportunidades para actividades delictivas y nuevas formas de delincuencia.

Hoy tenemos delitos informáticos que amenazan no solo la confidencialidad, la integridad, o la disponibilidad de los sistemas de computadoras, sino también a la seguridad de los seres humanos.

Llamamos seguridad informática al conjunto de medidas preventivas y reactivas que posibilitan la protección de la información con objeto de conseguir una elevada fiabilidad del sistema informático.

Es imposible garantizar la total seguridad de un sistema, por eso se habla de la fidelidad o confiabilidad como el grado de seguridad que se puede alcanzar en un sistema, una vez adaptando un conjunto de medidas.

Seguridad informática

Definir seguridad no es fácil, puesto que la seguridad se compone de varios elementos interrelacionados entre sí. **Los principales objetivos de la seguridad son:**

Confidencialidad (confidenciality): previene que individuos, entidades o procesos no autorizados puedan interpretar la información a la que no tienen derecho.

Integridad (Integrity): notifica contra posibles alteraciones no deseadas en la información, de modo que se garantice que el mensaje enviado en origen es exactamente el mensaje que se recibe en destino.

Disponibilidad (availability): mantiene la capacidad de exponer los activos informáticos utilizables en todo momento a los agentes autorizados que los consumen.

Seguridad Cibernética

Los objetivos secundarios:

Autenticidad y control de acceso: comprueba la identidad del agente que accede a un recurso y le facilita o deniega el acceso en función de esta identidad.

Fiabilidad: mantiene la consistencia entre el comportamiento del sistema y los resultados obtenidos del mismo, en otras palabras, evalúa si el sistema se comporta como se espera de él.

Irrenunciabilidad: garantiza la autoría de una información o un proceso.

Auditabilidad: registra el comportamiento del sistema para su evaluación posterior. Mediante políticas, controles de seguridad, tecnologías y procedimientos que detectan amenazas y que tratan de evitar o disminuir los riesgos que conllevan estas amenazas, se establece la estrategia de seguridad.

Elementos de la Seguridad

SEGURIDAD

Debe conseguirse

- Autorización
- Confidencialidad
- Autenticación
- Disponibilidad
- Integridad

Hay que proteger de

- Amenazas lógicas
- Catástrofes
- Atacantes
- Amenazas físicas
- Fugas de información

Debe protegerse

- El software
- Las configuraciones
- Las personas
- El hardware
- Las comunicaciones
- Los datos

Protegemos con

- La detección
- La auditoría
- La prevención
- La recuperación y restauración
- La gestión de recursos
- Los datos

Seguridad Cibernética

Amenazas riesgos y ataques

Amenaza: son acciones que pretenden dañar el sistema en riesgo, por ejemplo: los virus, una mala actuación de un administrador de sistemas, un empleado descontento, entre otras.

Vulnerabilidad o brecha: es el grado de exposición del sistema amenazado a las amenazas de un atacante, por ejemplo: un fallo de programación podría representar una vulnerabilidad, los sistemas son más vulnerables si no tienen antivirus o están actualizados con los parches recomendados por el fabricante.

Contramedida: acción que pretende la prevención de una amenaza que actúa aprovechándose de una vulnerabilidad. Por ejemplo: el administrador del sistema puede definir una política de actualización diaria del antivirus.

Atacante: agente activo que perpetra la amenaza que subyace a una vulnerabilidad.

Riesgo: es la valoración del daño que presentan las amenazas a las que está expuesto debido a las vulnerabilidades, tomando en cuenta las contramedidas que se implementan para la defensa.

Ante los riesgos se debe:

Evitar el riesgo: se evitan cuando se rechaza aceptarlos, o no se acepta ningún tipo de exposición, lo que exige compromiso de no realizar nunca la acción que origina el riesgo. Por ejemplo: para evitar el contagio de un virus de una llave USB, tenemos que deshabilitar los puertos USB y/o prohibir el acceso a la organización con estos dispositivos.

Reducir el riesgo: a veces los riesgos no se pueden evitar, pero si reducir a un mínimo asumible. Por ejemplo: se habilitan los puertos USB para que se puedan usar las memorias USB, pero a la vez mantenemos antivirus actualizados, lo que no evita el riesgo totalmente, pero si lo minimiza.

Retener, asumir o aceptar el riesgo: se acepta el riesgo y se asumen sus consecuencias en caso de que ocurra. Por ejemplo: si nos infectamos con un virus a través de una memoria USB por no tener antivirus, tendremos que asumir limpiezas periódicas de los sistemas, puesto que si no los protegemos se contaminarán frecuentemente.

Transferir o compartir el riesgo: buscar un respaldo y compartir el riesgo con otros controles o entidades. Por ejemplo: si se produce una infección por virus, una empresa

externa nos solucionará el problema o en dado caso de contar con un seguro, la compañía de seguros nos compensará la pérdida económica producida por el ataque.

Tipos de amenazas

Conocer las amenazas es fundamental para poder combatirlas, existen muchos tipos, a continuación enumeramos algunas de ellas:

Dependiendo del lugar de procedencia:

- Amenazas internas- vienen del interior del sistema atacado. Por ejemplo: de un miembro del Capital Humano de la organización que utiliza su puesto de trabajo para realizar un ataque.
- Amenazas externas- viene de fuera del sistema. Por ejemplo: el robo del servidor, una inundación, un hacker desde internet.

Dependiendo la vía de ataque:

- Amenazas físicas o ambientales: afectan al hardware o a las instalaciones en donde se ubica. Por ejemplo: una inundación, un fuego o robo.
- Amenaza lógica: afectan al sistema en su software mediante la introducción de malware o por la ejecución de operaciones lógicas que comprometen la seguridad del sistema. Por ejemplo: un troyano o un virus.

Riesgos de Seguridad Cibernética

Botnets: son cada vez más especializadas, dirigidas y peligrosas. Los criminales cibernéticos saben que estas herramientas son sus mejores activos y seguirán invirtiendo mucho tiempo, tecnología y fondos en ellos. Ahora llegan a estar más presentes a través de la variedad creciente de plataformas y se distribuyen con facilidad en casi todos los sistemas.

BYOD: Bring Your Own Device (traiga su propio dispositivo) es un fenómeno cada vez más difícil de controlar en el lugar de trabajo ya que hay cada vez más dispositivos que se pueden conectar a Internet. Las oficinas está llenas de dispositivos Android, iPhones, iPods y una gran variedad de tabletas y otros dispositivos que pueden actuar como puertas de acceso a los hackers experimentados. Los usuarios de estos dispositivos generalmente no entienden completamente los riesgos a los que están expuestos y a los que exponen a las organizaciones donde trabajan.

La nube: cada día más empresas recurren a este tipo de sistemas por su flexibilidad y capacidad para almacenar grandes cantidades de información. Sin embargo, son un gran atractivo para los hackers.

Seguridad Cibernética

Las APTs: Amenazas Persistentes Avanzadas (APT) son ataques dirigidos contra empresas u organizaciones para tratar de robar y filtrar información sin ser identificados. Por lo general, con la ayuda de ingeniería social, van poco a poco rompiendo las barreras de seguridad hasta infiltrarse en la red interna. Los ataques APT pueden ser muy difíciles de detectar, principalmente porque se dirigen a los servidores y actúan muy lentamente y fuera de los horarios de trabajo pico.

Medios Sociales: son la principal amenaza debido a su creciente popularidad y diversidad. Facebook, Twitter, LinkedIn y otras plataformas, los hackers tienen acceso a un sinnúmero de rutas de ataque. Las redes sociales conectan a las personas, pero a través de las cadenas de amigos y conocidos, acompañados de un perfil convincente y solicitudes de amistad inesperadas, pueden convertirse en fugas de información y con la ayuda de un sistema de seguridad deficiente, pueden derribar incluso las grandes empresas.

Riesgos internos: los expertos en seguridad saben que algunos de los ataques cibernéticos más peligrosos provienen del interior. Estos ataques pueden tener un efecto devastador, sobre todo porque un usuario privilegiado sabe qué datos usar o destruir. Las zonas más vulnerables son las instituciones financieras, como los bancos y las bolsas de valores.

Malware: ha sido durante mucho tiempo una poderosa herramienta utilizada por muchos hackers expertos. Pero el nuevo peligro viene del malware de precisión dirigida, un tipo evolucionado de ataque de malware. Su técnica ha mejorado en gran medida, los objetivos son más específicos y están diseñados para atacar configuraciones y componentes específicos. Los sistemas más vulnerables son las plataformas de medios sociales, incluyendo sus respectivas cuentas y grupos, dispositivos móviles y servidores remotos.

La seguridad de la información requiere la implementación de estrategias para cada uno de los procesos en donde debe tenerse en cuenta que la información es el activo primordial que debe protegerse.

Referencia:

Abad, A. (2013). Seguridad y Alta Disponibilidad. (1º Edición)España. Ibergarceta Publicaciones.

Brookshear, J. (1995). Introducción a las ciencias de la computación. Editorial Addison Wesley.

Gralla, P. (2008). Cómo Funciona Internet. Editorial Anaya Multimedia.

Negroponte, N. (1996). Ser digital. Editorial Océano

Vasconcelos, J. (2011). Introducción a la Computación. (3º Edición). México. Grupo Editorial Patria.

Vasconcelos, J. (2015). Tecnologías de la Información. (Segunda Edición). México, Grupo Editorial Patria.